Central Authentication

Network Infrastructure Equipment

Summer 2012

Reza Hajizadeh

hajjizadeh@gmail.com

problem statement

Considering the extent of today's networks, the use of remote communication tools to manage, configure and control network equipment is inevitable. Of course, this type of communication, in addition to facilitating and speeding things up, is a challenging issue that takes the mind of every network manager. has been busy Who has access? What is each user [1]allowed to do? What commands did each user execute during the connection? These are the most important questions that the network security manager must answer and adopt a method to implement them.

One of the most important issues to consider is the authentication method and the level of access of authorized people. In order to remotely connect to Cisco equipment, at least one username and password must be defined. There are two solutions for storing username/password:

1- Local database of each device
2- A central server

The use of the first method is justified for networks with a limited number of devices, but suppose that it is necessary to change an additional username or a password for a large number of switches and routers, in this case, the use of the second method is affordable. It is economical and more reliable [2].

[1]- When talking about the network management level, the user means the same as the network manager.

[2]- Because the settings are not repeated once for each device, there is no possibility of human error while typing the username/password.

Description of the current situation

Currently, the local database of each device is used completely independently for remote connection to switches and routers.

There are several solutions for using a local database:

1- Use a unique password for each device
The advantage of this method is to maintain more confidentiality and security for the devices. If the password of one of the devices is revealed, it is not possible for the attacker to connect to other devices.
The disadvantage of this method is when the number of equipment is large. In this case, since it is difficult to remember this number of passwords, it is necessary to write them down in a notebook, which also has its own risks.

2- Use a single password for all devices
This method does not have the disadvantage of the previous mode, but instead it has a bigger disadvantage that if the attacker has access to the password, he can also connect to all the equipment.

In the current network, a combination of the above two modes is used in such a way that the infrastructure equipment is divided into several groups (central core equipment, head office switches, city branch switches, routers abroad) and for each group username-word A unique pass is assigned.

Available solutions

The only reasonable and logical solution that does not have any of the disadvantages of the currently used method is to use a centralized server for authentication.

There are two protocols to implement this method:

1- RADIUS
2- TACACS

At the time of authentication, the action mechanism of both protocols is the same:

1- The user sends a remote communication request to the switch/router.
2- The username-password prompt will appear.
3- The username and password entered by the user are sent to the server.
4- The result (connection acceptance/rejection) is issued and sent to the switch/router.

It is necessary to explain that each of these protocols, in addition to authentication, also provides other capabilities to the network manager:

1- Granting different access rights to different users
Unique access can be created for network managers who work in different organizational units according to the work needs of that unit.[3]
2- Reporting of the commands that the user types and applies in the CLI[4]

[3]- **Organization** Unit
[4]- **Command Line** Interface

Advantages/disadvantages of the proposed methods

Table number 1 is a comparison of these two servers:

Features	RADIUS	TACACS
Layer 4 protocol	UDP	TCP
Encrypt transmission	Only Password	Entire session
Privilege modes support	Limited	15
Standard	Open Standard	Cisco Proprietary
Switch Memory Usage	Less	More than RADIUS
Architecture	Combine Authentication and Authorization	Separate AAA[5]
Authentication method	Local, LDAP Server	Local, LDAP Server, Active Directory

Table number 1 - Comparison of RADIUS and TACACS

conclusion

As it can be deduced from Table 1 , the TACACS protocol is superior to its competitor.

Regarding the reporting of orders, it is necessary to mention this point:

> Consider a situation where two users are making settings on the same device at the same time. If you do the reporting with the RADIUS protocol, it is not possible to separate the commands based on the user name, while this separation is possible using the TACACS protocol.

TACACS + server to use the AAA feature of Cisco equipment and to use the existing LDAP server for authentication .

According to the current conditions of the company and the right of access policy, it is possible to make an arrangement so that branch experts have access to a limited number of command line commands of the switches, such as show, debug , and can view reports to fix errors.

Considering that the reports of the switch are sent to the Syslog server , the report of the commands applied on the switch should be transferred to the same TACACS + server.

[5]- **A** authentication **A** uthorization **A** ccounting

Details of the proposed implementation

Required hardware: a physical/virtual server with the following minimum specifications:

- CPU: 3 GHz
- RAM: 2GB
- HDD: 30 GB

Protocol type: tacacs

Server: One of the open source software servers[6]

Authentication mechanism: use existing LDAP server

are connected to the central network at the company level or through layer 2 tunnel protocols .

Security mechanism: operating system security such as installing the latest updates, removing unnecessary services, and using an access control list [7]that allows only the management VLAN of the switches to access the server and through the [8]central distribution layer switch on network traffic is applied

[6]- Open Source
[7]- Access Control List (ACL)
[8]- Distribution Layer